ORIGINAL

BY FAX

Jonathan Shub, Esquire
Cal. Attorney I.D. No. 237708
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Phone: (215) 564-2300
Fax No. (215) 851-8029
Email: jshub@seegerweiss.com

Gary E. Mason (pro hac vice)
gmason@wbmllp.com
Donna F. Solen (pro hac vice)
dsolen@wbmllp.com
Jason S. Rathod (pro hac vice)
jrathod@wbmllp.com
WHITFIELD BRYSON & MASON LLP
1625 Massachusetts Ave., NW
Washington, DC 20036
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

Jamie E. Saltzman Weiss
Complex Litigation Group LLC
513 Central Avenue
Suite 300
Highland Park, IL 60035
Telephone: (847) 433-4500
Facsimilie: (847) 433-2500

Attorneys for Plaintiffs and the Proposed Class

Paid NP 99

Filed

APR 16 2012

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

ADR

E-filing

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CV12-01890 HRL

KENNETH CASSINE, VISHAL SHAH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., SAMSUNG ELECTRONICS AMERICA, INC., SAMSUNG TELECOMMUNICATIONS, AMERICA, LLC, HTC, Inc., HTC America, Inc., Sprint Nextel Corporation, and AT&T, Inc.

Defendants

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs KENNETH CASSINE, JANET RATHOD, and VISHAL SHAH, by and through their attorneys, allege on personal knowledge as to all facts related to themselves and on information and belief as to all other matters, which are based upon, among other things, the investigation made by Plaintiffs through their counsel and personal knowledge, as follows:

PRELIMINARY STATEMENT

1. This is a class action lawsuit, brought by, and on behalf of, a nationwide class of individuals whose privacy rights were violated by the collection, storing, and transmission of private data by software designed, sold and run by Carrier IQ, Inc. ("CIQ") that was imbedded without users' knowledge in phones manufactured by Samsung Electronics America, Inc., Samsung Telecommunications America, LLC (Samsung entities collectively referred to as "Samsung"), HTC, Inc., and HTC America, Inc. (HTC entities collectively referred to as "HTC") and serviced by Sprint Nextel Corporation ("Sprint") and AT&T, Inc. ("AT&T").

2. The software, which collects and stores phone user information and then transmits it to CIQ computer servers where the information is analyzed and transmitted to phone manufacturers and phone carriers, has been secretly installed on 150 million phones.

3. CIQ collected, stored and transmitted private data belonging to phone users without the users' knowledge or authorization. This information included some or all of the following: web-based searches conducted, the URLs of websites visited, videos watched, applications used, bank accounts accessed, the location of the user of the phone even when the customer has expressly denied permission for an application that is currently running to access his or her location, the phone numbers of senders of text messages and phone calls placed to the user, and the phone numbers of recipients of text messages and phone calls placed by the user.

4. The information stored on CIQ's software on users' phone handsets is transmitted roughly once a day to CIQ's servers. The information, then, is digested and transmitted to phone manufacturers and phone service providers.

5. CIQ's chief marketing officer Andrew Coward has recently admitted that CIQ holds a "treasure trove" of sensitive user information. David Kravets, "Carrier IQ Admits Holding 'Treasure Trove' of Consumer Data, But No Keystrokes," Wired, December 2, 2011,

available at http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/ (last accessed Dec. 05, 2011). In marketing materials on CIQ's website, CIQ boasts of its software's ability to enable businesses to "[s]ee which content [phone users] consume, even offline" and lists features of its software such as "[c]apture a vast array of experience data including screen transitions, button presses, service interactions and anomalies," "[a]nalyze data in real time, including comparative and cross correlation analysis across groups, geographies, devices and services," and "[v]iew application and device feature usage, such as camera, music, messaging, browser and TV." Carrier IQ, "IQ Insight Experience Manager," 2009, *available at* http://www.carrieriq.com/overview/IQInsightExperienceManager/ExperienceManager.datasheet.pdf (last accessed Dec. 05, 2011).

6. Phone users are unable to find or uninstall CIQ's software without highly sophisticated knowledge. For example, users could switch out their present operating system by "rooting" their phone and flashing an alternative operating system. This method, however, generally voids a phone's warranty.

7. Defendants' use of CIQ's software for the collection, storage, and transmission of private user data violates users' rights under the Federal Wiretap Act, the Federal Computer Fraud and Abuse Act, the Federal Stored Communications Act, and California common law.

JURISDICTION AND VENUE

8. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1331 for deprivation of rights guaranteed under the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* This Court also has jurisdiction pursuant to 28 U.S.C. § 1367(a) over Plaintiffs' state common law claims. Jurisdiction is also founded upon 28 U.S.C. § 1332(d) in that this is a putative class action with more than 100 class members, more than $5 million in controversy, and minimal diversity of citizenship.

9. Venue is appropriate pursuant to 28 U.S.C. § 1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations alleged in this complaint occurred in this District. Defendant CIQ, and its computer servers, reside here as CIQ maintains its

principle office and headquarters in this District.

PARTIES

10. Plaintiff Kenneth Cassine is an adult domiciled in Leesburg, Va. Mr. Cassine has owned and used phones manufactured by Samsung and HTC and serviced by Sprint. He currently owns and uses a Samsung phone serviced by Sprint.

11. Plaintiff Janet Rathod is an adult domiciled in Washington, D.C. Ms. Rathod has owned and used phones manufactured by Samsung and HTC and serviced by Sprint. She currently owns and uses a Samsung phone serviced by Sprint.

12. Plaintiff Vishal Shah is an adult domiciled in Washington, D.C. Mr. Shah owns and uses a Samsung phone serviced by AT&T.

13. Defendant Carrier IQ, Inc. is a Delaware corporation headquartered at 1200 Villa Street #200, Mountain View, CA 94041. CIQ is a provider of mobile services intelligence solutions to the wireless phone industry. It does business throughout the United States, and in particular, does business in the State of California and in this district.

14. Defendant Samsung Electronics America, Inc. is a New York corporation based in Ridgefield Park, NJ.

15. Defendant Samsung Telecommunications America, LLC is a Delaware limited liability company based in Richardson, TX.

16. Defendants HTC, Inc. and HTC America are Washington corporations based in Bellevue, Washington.

17. Defendant Sprint is a Kansas corporation based in Overland Park, KS.

18. Defendant AT&T is a Delaware corporation based in Dallas, TX.

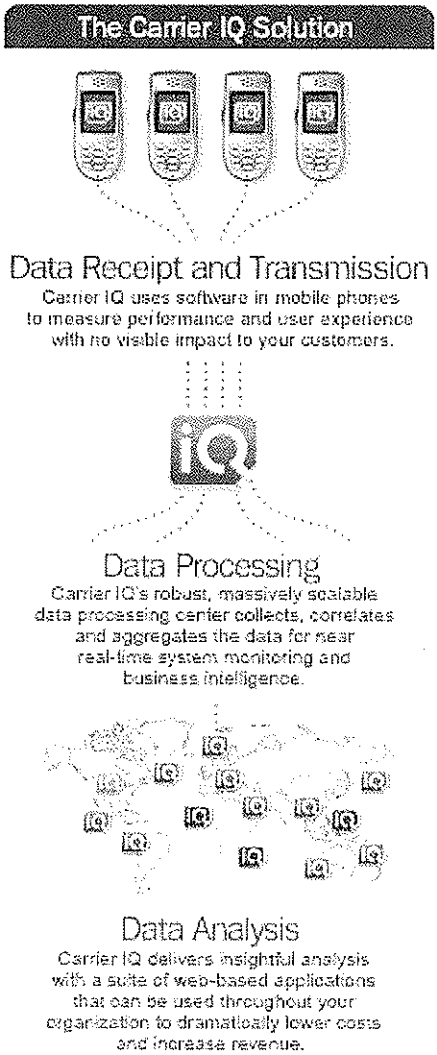
STATEMENT OF COMMON FACTS

19. CIQ is the leading provider of mobile services intelligence solutions to the wireless industry. It is a privately held corporation that was founded in 2005.

20. CIQ's professed aim is to supply mobile phone manufacturers and phone carriers with a wealth of granular, individual data on service performance and usability, enabling manufacturers and carriers to deliver higher quality products and services to their customers.

21. CIQ has sought to achieve its business mission by embedding software within 150 million phones. This software logs phone user information on the handset itself and is designed to be hidden from the user. The software then transmits the information to CIQ, phone manufacturers, and phone carriers on a daily basis.

22. On its website, CIQ graphically depicts its business model of collecting, storing and transmitting phone users' data as follows:



Carrier IQ, "Maximize Service. Minimize Churn," 2011, *available at* http://www.carrieriq.com/overview/index.htm (last accessed Dec. 04, 2011).

23. The data that CIQ collected, stored and transmitted was done without the users' knowledge or authorization. This information included some or all of the following: web-based

searches conducted, the URLs of websites visited, videos watched, applications used, bank accounts accessed, the location of the user of the phone even when the customer has expressly denied permission for an application that is currently running to access his or her location, the phone numbers of individuals who sent text messages and/or placed phone calls to the user, and the phone numbers of individuals who received text messages and/or phone calls placed by the user.

24. CIQ's chief marketing officer Andrew Coward has recently admitted that CIQ holds a "treasure trove" of sensitive user information. David Kravets, "Carrier IQ Admits Holding 'Treasure Trove' of Consumer Data, But No Keystrokes," Wired, December 2, 2011, *available at* http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/ (last accessed Dec. 05, 2011). In marketing materials on its website, CIQ boasts of its software's ability to enable businesses to "[s]ee which content [phone users] consume, even offline" and lists features of its software such as "[c]apture a vast array of experience data including screen transitions, button presses, service interactions and anomalies," "[a]nalyze data in real time, including comparative and cross correlation analysis across groups, geographies, devices and services," and "[v]iew application and device feature usage, such as camera, music, messaging, browser and TV." Carrier IQ, "IQ Insight Experience Manager," 2009, *available at* http://www.carrieriq.com/overview/IQInsightExperienceManager/ExperienceManager.datasheet.pdf (last accessed Dec. 05, 2011).

25. Mr. Coward has also specifically admitted to CIQ's practice of collecting, storing, and transmitting the URLs that phone users visit. David Kravets, "Carrier IQ Admits Holding 'Treasure Trove' of Consumer Data, But No Keystrokes," Wired, December 2, 2011, *available at* http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/ (last accessed Dec. 05, 2011). By obtaining the information directly from phone handsets, CIQ is able to collect URLs that would ordinarily be encrypted. One writer underscored the privacy concerns article on the topic, pointing out that "[s]ince the company is getting the URLs from the phone, they are able to record encrypted search terms such as https://www.google.com/#hl=en&sugexp=ppwe&cp=3&gs_id=p&xhr=t&q=abortion+clinics. By

contrast, your carrier, which sits between you and the internet, would normally only see https://www.google.com/ — for encrypted searches." *Id.*

26. CIQ's practices did not come to public light until December 2011 when a security researcher produced a video revealing the nature and operation of CIQ's software.

27. Phone users are unable to find or uninstall CIQ's software without highly sophisticated knowledge. For example, users could switch out their present operating system by "rooting" their phone and flashing an alternative operating system. This method, however, generally voids a phone's warranty.

28. Defendant Samsung has admitted that at least some of its cellular phones contain CIQ's software. It has said that the software is included in its phones when the phone carrier requests it.

29. Defendant HTC has admitted that at least some of its cellular phones contain CIQ's software. It has said that the software is included in its phones when the phone carrier requires it.

30. Defendant AT&T has admitted that it uses CIQ software, but alleged that it is used only to improve wireless network and service performance.

31. Defendant Sprint has admitted that it uses CIQ software, but alleged that it is used only to analyze network performance, identify areas where Sprint should be improving service and to understand device performance.

CLASS ALLEGATIONS

32. Plaintiffs brings this complaint on behalf of themselves and the class of all United States residents who have owned and operated a wireless phone device manufactured by and/or distributed by at least one Defendant manufacturer – HTC or Samsung – and serviced by at least one of the Defendant wireless phone carriers – AT&T or Sprint – from which Carrier IQ, Inc. had installed software that collected, stored, and transmitted electronic communications to any of the Defendants or third parties.

33. The members of the putative class are so numerous that joinder of individual claims is impracticable. CIQ software has been installed in 150 million phones.

34. There are significant questions of fact and law common to the members of the class. These issues include: whether the CIQ software collected, stored, and transmitted user information and if so, what user information the software shared and how; whether CIQ, the phone manufacturer Defendants (Samsung and HTC), and the phone carrier Defendants (Sprint and AT&T) failed to provide adequate information and opt out procedures for its users; whether by committing these acts and omissions, CIQ, the phone manufacturer Defendants and phone carrier Defendants violated federal and state laws; and whether class members are entitled to injunctive, declarative and monetary relief as a result of Defendants' conduct.

35. Plaintiffs' claims are typical of the claims of the putative class. Plaintiffs and all members of the putative class have been adversely affected and damaged in that CIQ software collected, stored, and transmitted their private information without the class members' knowledge or consent.

36. The proposed class representatives will fairly and adequately represent the putative class because they have the class members' interest in mind, their individual claims are co-extensive with those of the class, and because they are represented by qualified counsel experienced in class action litigation of this nature.

37. A class action in this instance is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of all members of the putative class is impracticable. Many members of the class are without the financial resources necessary to pursue this matter. Even if some members of the class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning the actions of CIQ, the phone manufacturer Defendants (Samsung and HTC), and the phone carrier Defendants (AT&T and Sprint) toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economy of scale and comprehensive supervision over the entire controversy by a single court.

38. The putative class may be certified pursuant to Rule 23(b)(2) of the Federal Rules

of Civil Procedure because Defendants have acted on grounds generally applicable to the putative class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the class.

39. The putative class may be certified pursuant to Rule 23(b)(3) of the Federal Rules of Civil Procedure because questions of law and fact common to class members will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

COUNT ONE

(Stored Electronic Communications Act, 18 U.S.C. § 2701 *et seq.*)

40. Plaintiffs repeat and reaffirm the assertions of fact contained in paragraphs 1 through 39 above.

41. The Stored Electronic Communications Act ("SECA") provides a cause of action against a person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system. 18 U.S.C. § 2701 *et seq.*

42. "Electronic Communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

43. "Electronic Storage" is defined in the statute to be "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17).

44. A user's private data, including web-based searches conducted, the URLs of websites visited, videos watched, applications used, bank accounts accessed, the phone numbers of individuals who sent text messages and/or placed phone calls to the user, the location of the user of the phone even when the customer has expressly denied permission for an application that

is currently running to access his or her location, and the phone numbers of individuals who received text messages and/or phone calls placed by the user, are electronic communications within the meaning of 18 U.S.C. § 2510(12).

45. Defendants hold the phone users' private data in electronic storage. 18 U.S.C. § 2510(17).

46. Defendants intentionally placed software on users' mobile devices that accessed their stored electronic communications without authorization.

47. By sharing users' information without consent from its users, Defendants knowingly divulge the contents of users' electronic communications while those communications are in electronic storage in violation of 18 U.S.C. §2702(a)(1).

48. By engaging in the foregoing acts and omissions, Defendants knowingly divulge the contents of users' electronic communications that are carried and maintained by Defendants on behalf of, and received by transmission from, users of Defendants' software in violation of 18 U.S.C. § 2702(a)(2).

49. By engaging in the foregoing acts and omissions, Defendants divulge its users' electronic communications to persons who are not the intended addressees or recipients. 18 U.S.C. § 2702(b)(1).

50. Defendants engage in the foregoing acts and omissions without obtaining the lawful consent of either the originators or the intended addressees or recipients. 18 U.S.C. § 2702(b)(3).

51. Defendants activated the information-divulging features of its software automatically, without providing the user any opportunity to opt-out and without obtaining any consent or authorization from the user.

52. None of the foregoing acts and omissions taken by Defendants are necessarily incident to Defendants' rendition of its software or to the protection of Defendants' rights or property. 18 U.S.C. § 2702(b)(5).

53. Because of the foregoing violations, Plaintiffs on behalf of the class are entitled to appropriate relief, including preliminary and other equitable or declaratory relief as this court

may deem appropriate. 18 U.S.C. § 2707(b)(1).

54. Plaintiffs on behalf of the class are entitled to a reasonable attorney's fee and other litigation costs reasonably incurred as provided by 18 U.S.C. § 2707(b)(3).

55. Defendants profit from the information-divulging aspects of CIQ's software. CIQ profits by marketing this software to phone manufacturers and phone carriers. Samsung and HTC profit by gaining the business of service providers such as Sprint and AT&T who require the installation of the software in phones they service. Sprint and AT&T profit by using the data improperly obtained to tailor its products and gain an advantage over competitors.

56. Plaintiffs on behalf of the class are entitled to recover monetary damages including actual damages, profits made by Defendants as described above, and statutory damages in the amount of not less than $1,000 per class member as provided by 18 U.S.C. § 2707(c).

57. Because Defendants' violations were willful and intentional, Plaintiffs on behalf of the class are entitled to recover punitive damages as provided by 18 U.S.C. § 2707(c).

COUNT TWO

(Wiretap Act, 18 U.S.C. §2510 *et seq.*)

58. Plaintiffs repeat and reaffirm the assertions of fact contained in paragraphs 1 through 57 above.

59. At all times relevant hereto, Plaintiffs and Class Members were persons entitled to the protection of 18 U.S.C. § 2511 as they were individuals who were party to electronic communications.

60. The Wiretap Act portion of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*, defines "electronic communication system" as any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

61. The Wiretap Act broadly defines the "contents" of a communication, when used with respect to any wire, oral, or electronic communications, to include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

"Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

62. Defendants' software (i.e., the software that collects, stores and transmits private data belonging to phone users without the users' knowledge or authorization roughly once a day to CIQ's servers, which is later transmitted to phone manufacturers and phone carriers) constitutes a device used to acquire the "contents" of communications, as that terms is defined 18 U.S.C. § 2510(5), in that the Defendants used the software to divert and transfer the substance, purport, and meaning of the communications to CIQ's servers as well as to phone manufacturers and phone carriers. Therefore, the software was used to "intercept" the contents of electronic communications, as that term is defined in 18 U.S.C. § 2510(4).

63. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting and endeavoring to intercept Plaintiffs and Class Members' wire and/or electronic communications to, from, and within their mobile devices through the use of the software.

64. Defendants also violated 18 U.S.C. § 2511(1)(d) by intentionally using, and endeavoring to use the contents of Plaintiffs and Class Members' wire and/or electronic communications to profit from its unauthorized collection and sale of Plaintiffs and Class Members' personal information, despite knowing and having reason to know, that the information was obtained through interception of an electronic communication in violation of 18 U.S.C. § 2511.

65. Defendants intentionally obtained, intercepted, used and/or intentionally endeavored to obtain, intercept and/or use, by device or otherwise, these wire and/or electronic communications, without the knowledge, consent or authorization of Plaintiffs and Class Members.

66. Defendants are not a party to any of the above-mentioned communications, nor have any of the parties to the communications given prior consent to Defendants' interception or divulging of those communications. 18 U.S.C. § 2511(2)(d).

67. Defendants installed and activated the information-divulging features of its

software automatically, without providing the user any opportunity to opt-out and without obtaining any consent or authorization from the user.

68. Because of the foregoing violations, Plaintiffs on behalf of the class is entitled to appropriate relief, including preliminary and other equitable or declaratory relief as this court may deem appropriate. 18 U.S.C. § 2520(b)(1).

69. Plaintiffs on behalf of the class are entitled to a reasonable attorney's fee and other litigation costs reasonably incurred as provided by 18 U.S.C. § 2520(b)(3).

70. Plaintiffs on behalf of the class are entitled to recover monetary damages in amounting to the greater of: (a) the sum of actual damages and any profits made by Defendants as a result of the violations of law caused by its software; or (b) statutory damages in the amount of $100 per day of violation per class member, up to a maximum amount of $10,000 per class member. 18 U.S.C. § 2520(c)(2).

COUNT THREE

(Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*)

71. Plaintiffs repeat and reaffirm the assertions of fact contained in paragraphs 1 through 70 above.

72. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers.

73. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA."

74. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

75. Each of the Plaintiffs and Class Members' mobile devices is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

76. Defendants violated 18 U.S.C. § 1030 by causing the transmission of a software

program to Plaintiffs and Class Members' mobile devices, which accessed the personal information of Plaintiffs and Class Members and transmitted such information to CIQ computer servers, phone manufacturers, and phone carriers.

77. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a software program to operate in Plaintiffs and Class Members' mobile devices, which are protected computers as defined above, and intentionally causing damage without authorization.

78. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs and Class Members' protected mobile devices without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs and Class Members' mobile devices by impairing the integrity of data and/or system and/or information.

79. Defendants intended to cause damage in that they knew or should have known that their conduct would consume Plaintiffs' and Class Members' valuable computer assets and resources.

80. Defendants intended to access Plaintiffs and Class Members' computers personal information, inasmuch as such access was accomplished through the execution of a software program specifically designed for such access, which effectuated access of Plaintiffs and Class Members' computers.

81. Defendants' conduct was without authorization and/or exceeding authorization.

82. Plaintiffs and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information," in that Defendants' conduct caused the condition, value and functionality of Plaintiffs and Class Members' mobile devices and their related computer resources to be impaired.

83. Plaintiffs and Class Members have suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other

consequential damages incurred because of interruption of service." As a result of Defendants' conduct, Plaintiffs and Class Members suffered costs incurred due to Defendants' utilization of their valuable computer resources, the diminution in value of their mobile devices, and the deprivation of the value of their information assets.

84. Defendants' unlawful access to Plaintiffs and Class Members' computers, use of their computer assets and resources, interruption of their services, and taking of their information was carried out through the same automated process, and resulted in an aggregated loss to Plaintiffs and Class Members of at least $5,000 within a one-year period.

85. The aggregated losses to Plaintiffs and Class Members amount to $5,000 or greater during a one-year period in that the diminution in the value of the mobile devices can be discerned through discovery of Defendants' record and expert testimony. When losses are aggregated across Plaintiffs and Class Members, losses exceed $5,000 during any one year period during the Class Period.

86. Defendants' unlawful access to Plaintiffs and Class Members' computers and electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs and Class Members' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

87. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and Class Members have suffered harm and are entitled to appropriate relief pursuant to 18 U.S.C. § 1030.

COUNT FOUR

(Public Disclosure Tort)

96. Plaintiffs repeat and reaffirm the assertions of fact contained in paragraphs 1 through 87 above.

97. By engaging in the forgoing acts and omissions, Defendants committed the common law tort of Public Disclosure of Private Facts as recognized by California common law.

Its software resulted in the public disclosure of private facts which would be offensive and objectionable to a reasonable person, and which facts are not of legitimate public concern.

PRAYER FOR RELIEF

98. **WHEREFORE** Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand judgment against Defendants as follows:

a. For an order certifying the Class proposed herein and appointing Plaintiffs and their counsel to represent the Class;

b. For a declaration that Defendants' acts and omissions constitute a knowing and unauthorized invasion of its users' privacy rights in violation of the laws of the United States and the State of California;

c. For preliminary and permanent injunctive relief enjoining and preventing CIQ's software program from continuing to operate in cellular phones in which it is installed without appropriate safeguards, default provisions and opt-in mechanisms to ensure that the private data of its users is not improperly disclosed or transmitted in the future;

d. For an award of damages, including without limitation damages for actual harm, profits made by Defendants in the operation of CIQ's software, and statutory damages where applicable;

e. For an award of reasonable attorneys' fees and costs incurred by Plaintiffs and the members of the putative class in prosecuting this matter; and

f. For an award of such other relief in law and equity to which Plaintiffs and the members of the putative class may be entitled.

DATED: April 16, 2012

By: /s/ Jonathan Shub

Jonathan Shub, Esquire
Cal. Attorney I.D. No. 237708
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Phone: (215) 564-2300
Fax No. (215) 851-8029
Email: jshub@seegerweiss.com

Gary E. Mason (pro hac vice)
Donna F. Solen (pro hac vice)
Jason S. Rathod (pro hac vice)
WHITFIELD BRYSON & MASON LLP
1625 Massachusetts Ave., NW
Suite 605
Washington, DC 20036
Phone: (202) 429-2290
Fax: (202) 429-2294
Email: gmason@masonlawdc.com
dsolen@masonlawdc.com
jrathod@masonlawdc.com

Jamie E. Saltzman Weiss
Complex Litigation Group LLC
513 Central Avenue
Suite 300
Highland Park, IL 60035
Telephone: (847) 433-4500
Facsimilie: (847) 433-2500

Attorneys for Plaintiffs and the Proposed Class